DEPARTMENT OF DEFENSE
UNITED STATES CYBER COMMAND
9800 SAVAGE ROAD, SUITE 6171
FORT GEORGE G. MEADE, MARYLAND 20755

FEB 1 0 2021

Runa Sandvik
MuckRock News
DEPT MR 106429
411A Highland Ave
Somerville, MA 02144-2516

Re: 21-R019

Dear Ms. Sandvik,

Thank you for your January 1, 2021, Freedom of Information Act (FOIA) request for material regarding "the creation of the 2020 ComRATv4 illustration" as seen on Twitter.

We have located and reviewed 21 pages of material responsive to your request. As the Initial Denial Authority, I have determined that the redacted information is exempt from disclosure under the FOIA, Title 5, United States Code, section 552(b)(1), (b)(3), (b)(5), and (b)(6). Enclosed are details of the specific exemptions cited.

If you are not satisfied with our action on this request, you may seek dispute resolution services from the DoD FOIA Public Liaison or the Office of Government Information Services. You also have the right to file an administrative appeal. Information about these services is enclosed.

DAVID T. ISAACSON
Major General, U.S. Army
Chief of Staff

Attachments:
Enclosure a/s

FOIA Exemptions Cited:

(b)(1) – information properly and currently classified in the interest of national defense or foreign policy, pursuant to Executive Order 13526, Classified National Security Information:

Section 1.4(a) – military plans, weapons systems, or operations

Section 1.4(c) – intelligence activities (including covert action), intelligence sources or methods, or cryptology

(b)(3) – information specifically exempted from disclosure by statute:

10 U.S.C. § 130b, personally identifying information of DoD personnel in sensitive units

10 U.S.C. § 130e, defense critical infrastructure security information

(b)(5) – inter- or intra-agency memoranda containing information that is deliberative and pre-decisional

(b)(6) – information in personnel and medical files and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy

DoD FOIA Public Liaison:

Ms. Melissa Walker
Phone: (571) 371-0462
Email: osd.foialiaison@mail.mil

Administrative Appeal:

Ms. Joo Chung
ODCMO Director of Oversight and Compliance
4800 Mark Center Drive
ATTN: DPCLTD, FOIA Appeals
Mailbox #24
Alexandria, VA 22350-1700
Email: osd.foia-appeal@mail.mil

* Appeal should cite case number above, be clearly marked "FOIA Appeal" and filed within 90 calendar days from the date of this letter.

Office of Government Information Services:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road – OGIS
College Park, MD 20740-6001
Email: ogis@nara.gov
Phone: (202) 741-5770
Toll Free: 1-877-684-6448
Fax: (202) 741-5769

(b)(3) 10 U.S.C. § 130b

[redacted]

From: [redacted] (b)(3) 10 U.S.C. §§ 130b, 130e
Sent: Wednesday, October 7, 2020 11:24 AM
To: [redacted]
Cc: [redacted]

[redacted] DL USCC_J0PAO (ALIAS) H3C020; [redacted]

[redacted]

Subject: (U) Public Disclosure Deconfliction Request
Signed By: [redacted]@cybercom.ic.gov

Importance: High

Classification: ~~TOP SECRET//SI//REL TO USA, FVEY~~

[redacted] (b)(3) 10 U.S.C. § 130e

Please forward to [redacted] and request deconfliction of the (2) malware samples below for public disclosure.

Intended date of disclosure is 29 OCT. Request **suspense NLT** [redacted].

1. **(~~TS//SI//REL~~)** [redacted] (b)(1) Sec. 1.4(a, c)
   a. Actor:
   b. Malware: [redacted]
2. **(U) Commercial Names for Actor and Malware**
   a. Actor: Turla
   b. Malware: ComRAT
3. **(U) Malware Sample File Names**
   a. pe64.dll
      i. MD5: 7431403594649a22b45320d311f23d28
      ii. SHA1: 04a4223fdee5dd2f55c68d8cb2e2e8c645ba7c14
      iii. SHA-256: 083be09ceecf0f8a5c6a48d105967b33522b531e04221850e671bfc5b2231313
   b. pe32.dll
      i. MD5: bdc11fd2408cae5e687aa9cef65f0221
      ii. SHA-1: c942a1615e14ae0c9cf13f47e13a856128a5d59f
      iii. SHA-256: 944f29926aee6d2cd3d0ddb0968f7db00837806adaa3a093b7175b2e973d0f57

[redacted]

(b)(3) 10 U.S.C. § 130b

Cyber National Mission Force, US Cyber Command
NSTS: 963-8780 | NSAnet: [redacted]@cybercom.ic.gov
VoSIP: [redacted] | SIPRnet: [redacted]@mail.smil.mil
PSTN: [redacted] | NIPRnet: [redacted]@mail.mil

Classified By: [redacted]
Derived From: NSA/CSSM 1-52
Dated: 20130930

(b)(3) 10 U.S.C. § 130b

From: (b)(3) 10 U.S.C. § 130b, (b)(6)
Sent: Tuesday, October 20, 2020 11:46 AM
To:
Cc: DL USCC_J0PAO (ALIAS) H3C020;
Subject: (U) Graphic Ad Hoc request from USCYBERCOM PA
Attachments: (b)(5)

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Good morning, graphic team extraordinaire-

BLUF: Requesting a quick turn of three graphics, as described, below. We are requesting the graphics NLT two days before the final request date, so we have time for commander review.

The POC for this is cc'd, but please coordinate with me as well!

(b)(3) 10 U.S.C. § 130b

(b)(5)

Graphic for use 26 Oct:

A graphic of . Objective is to release (b)(5)

(b)(3) 10 U.S.C. § 130e, (b)(5)

Graphics for use 28 and 29 Oct:

Graphic 1: malware public disclosure 28 OCT

Graphic concept: Cartoon bear in soviet uniform costume holding Halloween candy basket with malware names (ComRAT, Drovorub, WellMess, X-Agent, X-Tunnel, Lojax) on candy bars

Graphic 2: ComRAT malware public disclosure 29 OCT

Graphic concept: Image of same bear in soviet uniform costume holding Halloween candy basket, now tripping with "treats" (malware names) spilling out of candy basket

(U//~~FOUO~~)

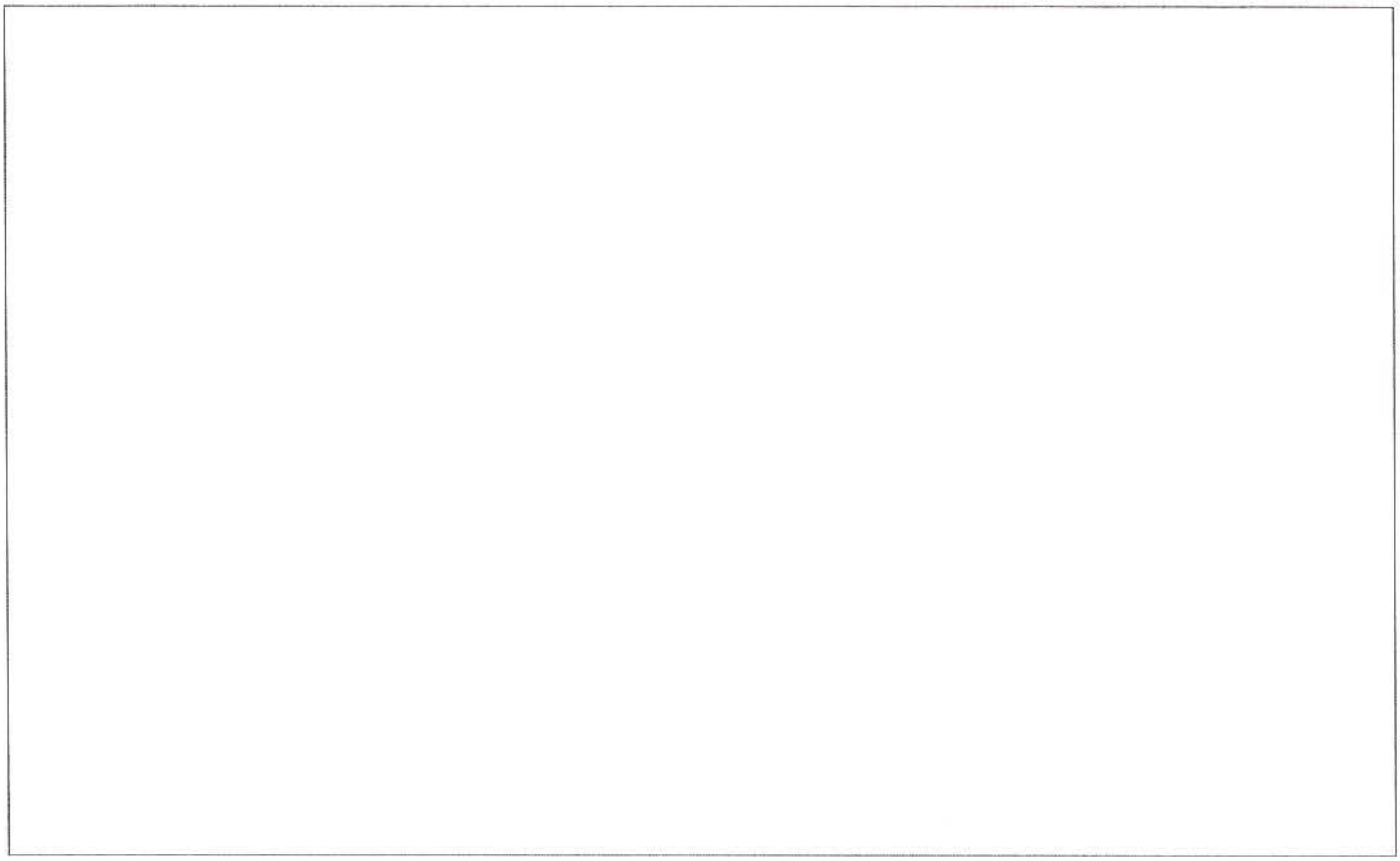
(b)(3) 10 U.S.C. § 130b

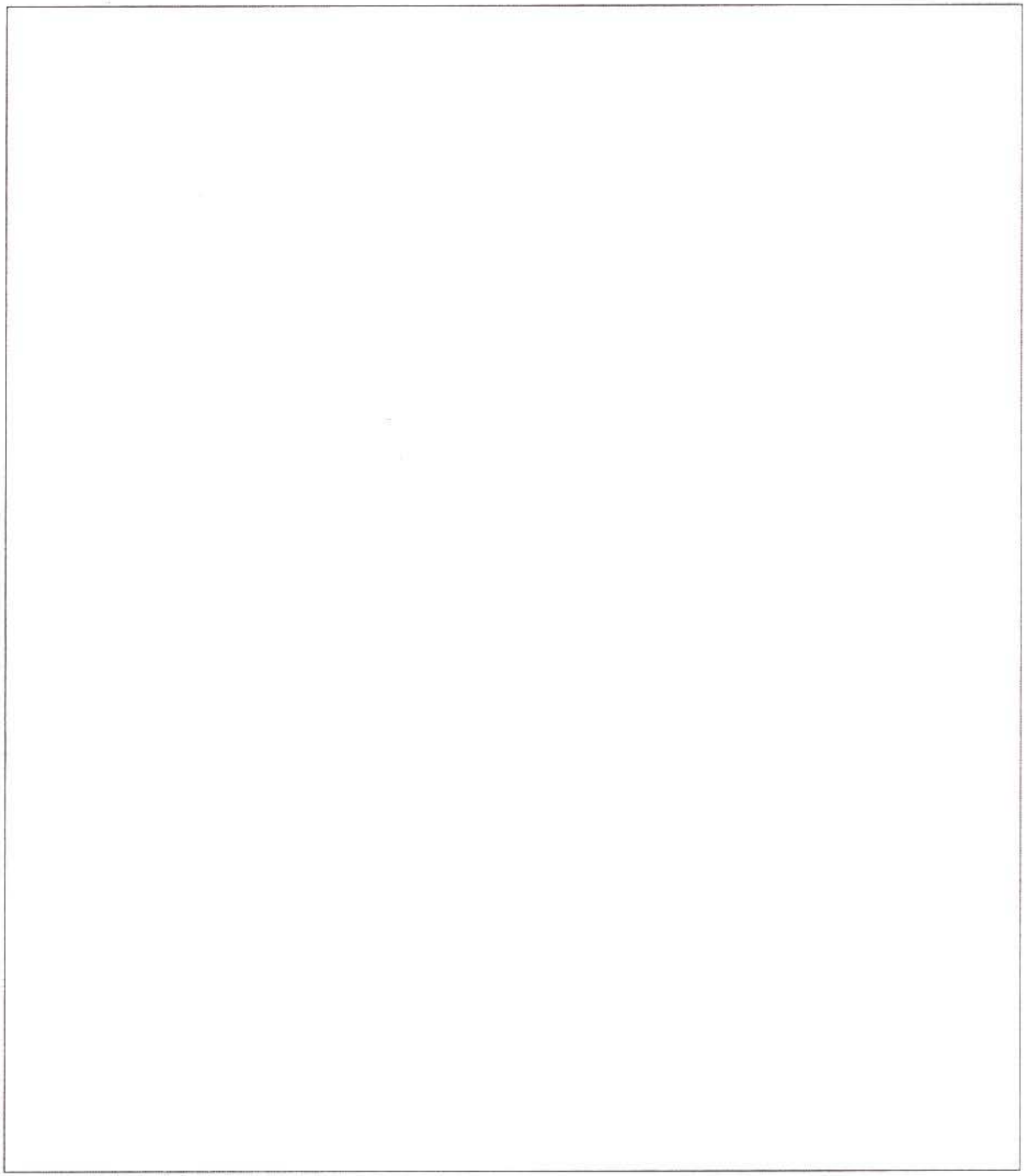
U.S. Cyber Command Public Affairs
NSTS: 969-3876

COMM: 240-373-8024
(U//~~FOUO~~)

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(b)(3) 10 U.S.C. § 130e, (b)(5)





(b)(3) 10 U.S.C. § 130e, (b)(5)

(b)(3) 10 U.S.C. § 130b

From: (b)(3) 10 U.S.C. § 130b, (b)(6)
Sent: Tuesday, October 20, 2020 1:15 PM
To:
Cc: DL USCC_J0PAO (ALIAS) H3C020;
Subject: RE: (U) Graphic Ad Hoc request from USCYBERCOM PA

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Good Afternoon (b)(3) 10 U.S.C. § 130b

Thank you for reaching out and providing this information. My team and I are very excited to create more graphics for you. I will coordinate with you and on this project.

(b)(3) 10 U.S.C. § 130b

Very Respectfully,

(b)(6)

(b)(3) 10 U.S.C. § 130b, (b)(6)

From: @nsa.ic.gov>
Sent: Tuesday, October 20, 2020 11:46 AM
To: @nsa.ic.gov>; @nsa.ic.gov>; @nsa.ic.gov>; @nsa.ic.gov>; @nsa.ic.gov>; @nsa.ic.gov>
Cc: @nsa.ic.gov>; @cybercom.ic.gov>; DL USCC_J0PAO (ALIAS) H3C020 @nsa.ic.gov>; @cybercom.ic.gov>; @nsa.ic.gov>; @cybercom.ic.gov>; @cybercom.ic.gov>; @nsa.ic.gov>; @nsa.ic.gov>; @cybercom.ic.gov>; @nsa.ic.gov>; @cybercom.ic.gov>; @cybercom.ic.gov>; @nsa.ic.gov>; @cybercom.ic.gov>; @cybercom.ic.gov>; @nsa.ic.gov>;

(b) (6)

[redacted]@nsa.ic.gov>
Subject: (U) Graphic Ad Hoc request from USCYBERCOM PA

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Good morning, graphic team extraordinaire-

BLUF: Requesting a quick turn of three graphics, as described, below. We are requesting the graphics NLT two days before the final request date, so we have time for commander review.

The POC for this is [redacted] cc'd, but please coordinate with me as well!

(b) (3) 10 U.S.C. § 130b

(b) (5)

Graphic for use 26 Oct:

A graphic of [redacted]. Objective is to release (b) (5)

[redacted]

(b) (3) 10 U.S.C. § 130e, (b) (5)

Graphics for use 28 and 29 Oct:

Graphic 1: [redacted] **malware public disclosure 28 OCT**

Graphic concept: Cartoon bear in soviet uniform costume holding Halloween candy basket with malware names (ComRAT, [redacted] Drovorub, WellMess, X-Agent, X-Tunnel, Lojax) on candy bars

Graphic 2: ComRAT malware public disclosure 29 OCT

Graphic concept: Image of same bear in soviet uniform costume holding Halloween candy basket, now tripping with "treats" (malware names) spilling out of candy basket

(U//~~FOUO~~)

(b) (3) 10 U.S.C. § 130b

[redacted]

U.S. Cyber Command Public Affairs
NSTS: 969-3876
COMM: 240-373-8024
(U//~~FOUO~~)

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(b)(3) 10 U.S.C. § 130b

From:
Sent: Thursday, October 29, 2020 10:34 AM (b)(3) 10 U.S.C. § 130e, (b)(5)
To: DL USCC_J0PAO (ALIAS) H3C020
Subject: FW: (U) FOR REVIEW: (U) 29 OCT_ and ComRAT MDP ComPlan
Attachments: ComRAT Graphic.jpg; Pumpkin Graphic.jpg
Signed By: @nsa.ic.gov

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Team-

For your media and social media analysis

(U//~~FOUO~~) (b)(3) 10 U.S.C. § 130b

United States Cyber Command, Public Affairs
NSTS: 969-2254
COMM: 667-812-3532 (b)(3) 10 U.S.C. § 130b
TELEWORKING:
(U//~~FOUO~~)

From: @cybercom.ic.gov> (b)(3) 10 U.S.C. § 130b, (b)(6)
Sent: Wednesday, October 28, 2020 4:41 PM
To: Hartman William J USA USA @cybercom.ic.gov>; @nsa.ic.gov>
Cc: @nsa.ic.gov>; @nsa.ic.gov>; @nsa.ic.gov>; @cybercom.ic.gov>; @cybercom.ic.gov>; @nsa.ic.gov>; @cybercom.ic.gov>; @cybercom.ic.gov>; @cybercom.ic.gov>; @nsa.ic.gov>; @nsa.ic.gov>; @nsa.ic.gov>; @nsa.ic.gov>; @nsa.ic.gov>; @nsa.ic.gov>; @nsa.ic.gov>; @nsa.ic.gov>; @nsa.ic.gov>; @nsa.ic.gov>; @nsa.ic.gov>; @nsa.ic.gov>; @nsa.ic.gov>; @cybercom.ic.gov>; @cybercom.ic.gov>; @nsa.ic.gov>; @cybercom.ic.gov>
Subject: RE: (U) FOR REVIEW: (U) 29 OCT_ and ComRAT MDP ComPlan
(b)(3) 10 U.S.C. § 130e, (b)(5)

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

BG Hartman,

In advance of the meeting, below is the latest we have and the graphics are attached for reference and review.

TIMELINE OF EVENTS

(b) (3) 10 U.S.C. § 130e

29OCT/1300 DHS/CISA posts ComRAT malware analysis report (MAR) to [INSERT LINK]

29OCT/1300 CNMF [ ] upload 3 malware samples to Virus Total. Operators will inform USCYBERCOM/CNMF public affairs when this occurs to ensure timely alignment.

VIRUS TOTAL DRAFT LANGUAGE:
(U) An implant dropper dubbed ComRAT v4 was just attributed to the Russian sponsored APT Turla. This malware has likely targeted victims such as ministries of foreign affairs and a national parliament. The malware exfiltrates sensitive documents, executes additional programs, and utilizes Gmail for C2.

For additional information, please see: https://twitter.com/CNMF_CyberAlert #CNMF"

29OCT/1300

Following are the actions USCYBERCOM plans to take when directed.

a) **Retweet @US-CERT *ComRAT MAR***

a) **Tweet 2, Day 2: *Updated Language highlighting ComRAT VT* uploads**
Drafted for the CNMF_CyberAlert Twitter account:

@CISAgov and @FBI attributed the latest sample of an implant dropper dubbed #ComRATv4 to, Russian APT, Turla. It has likely been used to target ministries of foreign affairs and national parliament.

See more on @CNMF_CyberAlert's Virus Total: [LINK]

a. (U) Request amplification by: DHS, FBI, NSA, EUCOM, State Dept

---

29OCT/1400 DHS/CISA posts malware analysis report (MAR) to [INSERT LINK]

(b) (3) 10 U.S.C. § 130e

29OCT/1400 CNMF [ ] uploads 2 malware samples to Virus Total. Operators will inform USCYBERCOM/CNMF public affairs when this occurs to ensure timely alignment.

VIRUS TOTAL DRAFT LANGUAGE:

These samples are the Stage 2 for this malware implant. This malware has likely been used to target victims in Eastern European and Central Asian countries to include embassies and ministries of foreign affairs.

For additional information, please see: https://twitter.com/CNMF_CyberAlert #CNMF"

Following are the actions USCYBERCOM plans to take when directed.

a) **Retweet: *Updated Language highlighting MAR***
Direct retweet from the CNMF_CyberAlert Twitter account:

b) **Tweet 2, Day 1: *Updated Language highlighting malware VT uploads***
Drafted for the CNMF_CyberAlert Twitter account:
(U) @CISAgov and @CNMF_CyberAlert released the latest MAR this #malware has likely been used to target embassies and ministries of foreign affairs in Eastern Europe and Central Asia.

See more on our Virus Total page: [LINK]

b. (U) Request amplification by: DHS, FBI, NSA, EUCOM, State Dept

29OCT1400 (U//~~FOUO~~) In support of this effort USCYBERCOM/PA will

---

(b) (3) 10 U.S.C. § 130e

31OCT/0900

Halloween Tweet: *Updated Language highlighting malware and ComRAT VT* uploads
Drafted for the CNMF_CyberAlert Twitter account:

#ICYMI, Latest ComRAT and malware sample uploaded to @CNMF_CyberAlert's virus total page. These samples have been used to target victims in Eastern Europe and Central Asia.

(b) (5)

(U//~~FOUO~~) If asked,

v/r,

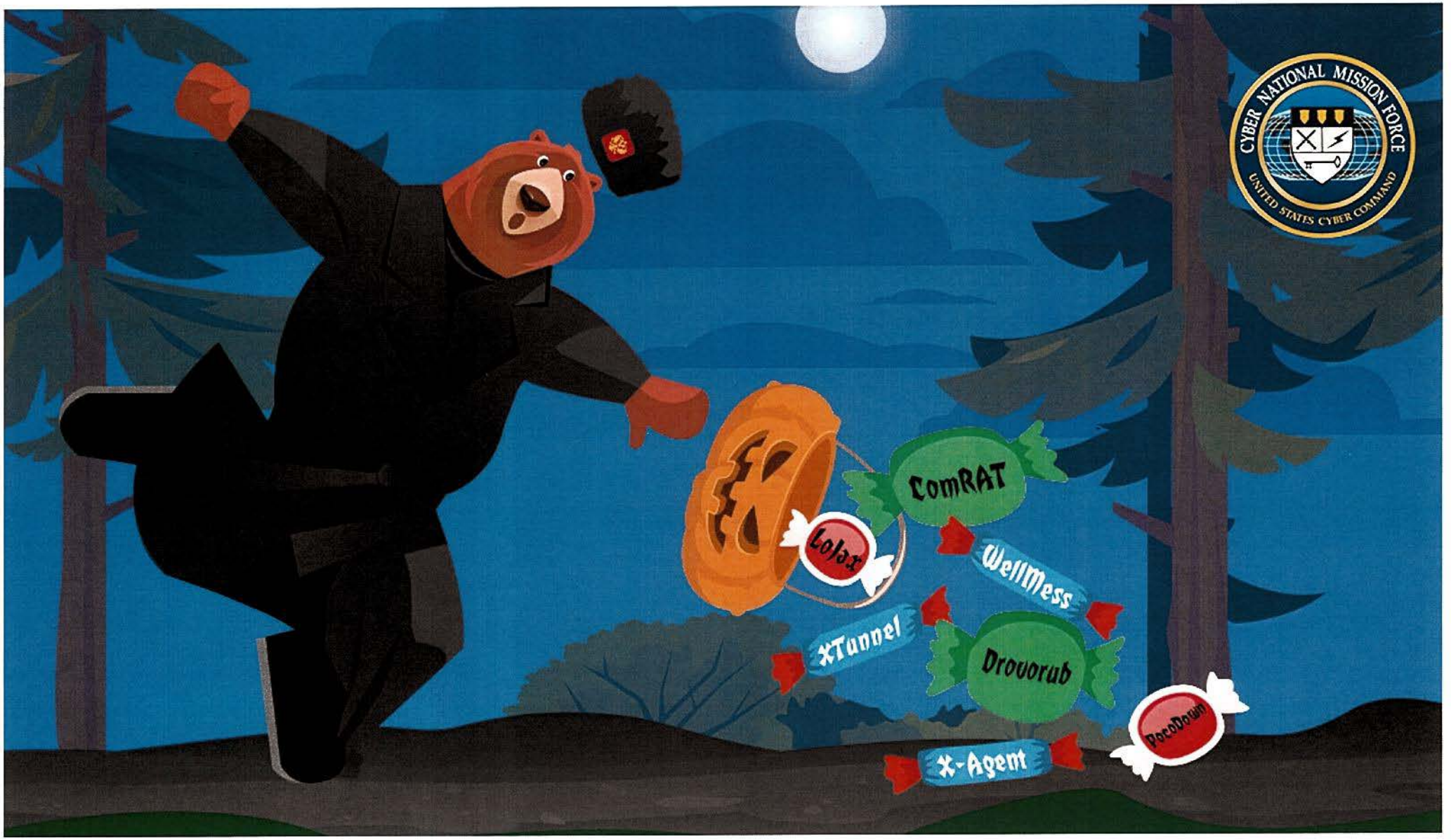
(b)(3) 10 U.S.C. § 130b

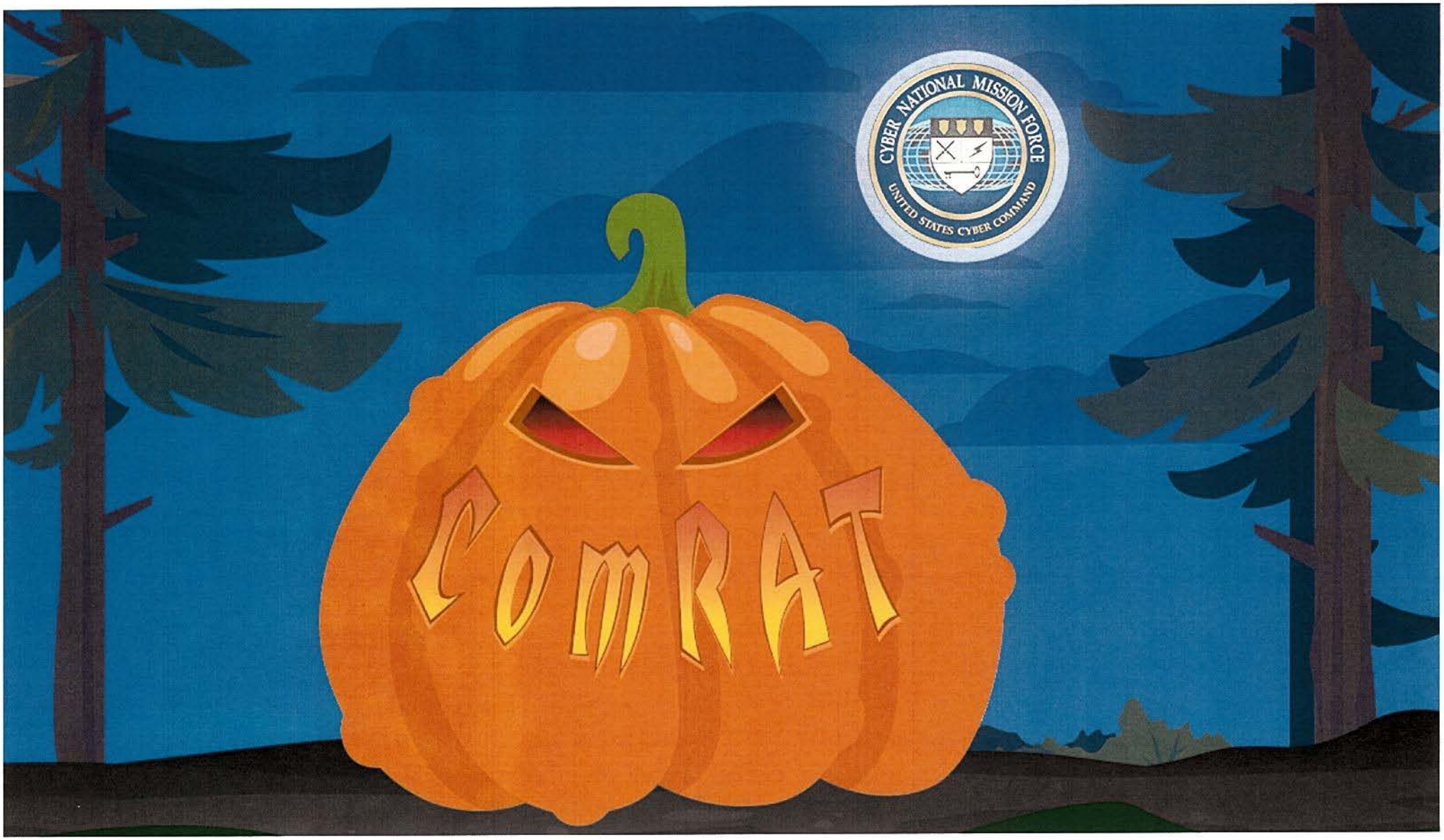
(U//~~FOUO~~)

Cyber National Mission Force, Public Affairs
United States Cyber Command
NSTS: 969-3107
COMM: 443-654-0239
(U//~~FOUO~~)

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~


CYBER NATIONAL MISSION FORCE
UNITED STATES CYBER COMMAND
ComRAT
Lolax
WellMess
xTunnel
Drovorub
PocDown
X-Agent


CYBER NATIONAL MISSION FORCE
UNITED STATES CYBER COMMAND
COMRAT

[redacted]

From: [redacted]
Sent: Thursday, November 12, 2020 5:24 PM
To: DL USCC_J0PAO (ALIAS) H3C020
Subject: FW: (U) How the Pentagon is trolling Russian, Chinese hackers with cartoons_Cyberscoop
Attachments: How the Pentagon is Trolling Russian and Chinese Hackers with Cartoons.docx

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

FYSA

(U//~~FOUO~~)
[redacted]
U.S. Cyber Command Public Affairs
NSTS: 969-3876
COMM: 240-373-8024
Building [redacted]
(U//~~FOUO~~)

From: [redacted]
Sent: Thursday, November 12, 2020 5:23 PM
To: DL USCC_LL_Staff (ALIAS) H3C [redacted]@nsa.ic.gov>; [redacted]@cybercom.ic.gov>
Subject: FW: (U) How the Pentagon is trolling Russian, Chinese hackers with cartoons_Cyberscoop

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

[redacted] and LL teammates-

FYSA, Cyberscoop published something on our use of graphics with malware disclosure- highlighting the trolling of adversaries. Likely a blip in the world of Congress, if anything...but wanted to make you aware.

(U//~~FOUO~~)
[redacted]
U.S. Cyber Command Public Affairs
NSTS: 969-3876
COMM: 240-373-8024
Building [redacted]
(U//~~FOUO~~)

From: [redacted]@cybercom.ic.gov>
Sent: Thursday, November 12, 2020 5:21 PM
To: Hartman William J USA USA [redacted]@cybercom.ic.gov>; [redacted]@nsa.ic.gov>
Cc: [redacted]@nsa.ic.gov>; [redacted]@nsa.ic.gov>; [redacted]@cybercom.ic.gov>; [redacted]@nsa.ic.gov>
Subject: FW: (U) How the Pentagon is trolling Russian, Chinese hackers with cartoons_Cyberscoop

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

BG Hartman,

BLUF: This afternoon, Cyberscoop released an article centered around USCYBERCOM and CNMF's use of graphics to amplify malware disclosures. The article, while a bit tongue and cheek, is mostly accurate and does highlight the core purposes of the malware disclosures.

- USCYBERCOM imposes costs on adversaries by disclosing their malware, to cut off their access and reinforce defenses
- Graphics are used and included to increase engagement and resonate within the Cybersecurity industry; sources also indicated intent to message adversaries
- The graphics may not be shaping adversary behavior but do tie into USCYBERCOM's Persistent Engagement strategy to 'bolster arsenal of responses'

Ms. Vavra also reached out to Cyber Command PA for comment and the name of the graphics company. CYBERCOM did not provide the name of the company but did provide the comment below:
Cyber Command spokesperson said the command "develops visual imagery to engage with the cyber security community on malware disclosures and vulnerability alerts. We recognize the key role that industry plays in ensuring global cybersecurity defense against malicious cyber actors, and so we leverage social media best practices to enhance messaging with industry."

Please let me know if you have any questions or concerns.

V/R,

(b)(3) 10 U.S.C. § 130b

(U//~~FOUO~~)

Cyber National Mission Force, Public Affairs
United States Cyber Command
NSTS: 969-3107
COMM: 443-654-0239
(U//~~FOUO~~)

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

GOVERNMENT

How the Pentagon is trolling Russian, Chinese hackers with cartoons

Written by Shannon Vavra

NOV 12, 2020 | CYBERSCOOP

There's little that Russian hackers hate more than being seen as soft. So when U.S. military hackers saw a way to publicly portray them as bumbling and unthreatening in recent weeks, they seized the moment.

It all began when Cyber Command, the U.S. Department of Defense's offensive cyber arm, started working with a graphics company to illustrate foreign government hackers. The military realized it could punch up the reports it releases on foreign hacking operations by adding illustrations, and try to embarrass or infuriate the foreign hacking shops along the way, one U.S. official told CyberScoop.

In one case, when Cyber Command started making plans to expose some state-sponsored espionage operations tied to Russia's Federal Security Service (FSB), the country's KGB successor, they turned to the graphics company to develop images that would goad the Russians, the official said.

"Russia hates to be seen as cuddly or cozy so we want to tick them off," said the official, who was not authorized to speak with the press.

The best way to do that, the military hackers decided, was to represent the FSB hackers as an endearing, if bumbling, bear. (The cybersecurity community has long used names

with references to bears to identify Russian hacking outfits, such as Cozy Bear and Fancy Bear, the hacking groups behind the 2016 breach of the Democratic National Committee.)

An implant dropper dubbed #ComRATv4 recently attributed by @CISAgov and @FBI to Russian sponsored APT, Turla. It was likely used to target ministries of foreign affairs and national parliament.
@CNMF_CyberAlert continues to disclose #malware samples
on: https://t.co/fSgk1xpG8t pic.twitter.com/c2jmozTAyB

— USCYBERCOM Cybersecurity Alert (@CNMF_CyberAlert) October 29, 2020

Art that the cybersecurity community uses to portray Russian hackers has typically shown burly or ferocious bears, but Cyber Command wanted to avoid giving the Russian hackers an ego boost, the official said.

"We don't want something they can put on T-shirts," the U.S. official said. "We want something that's in a PowerPoint their boss sees and he loses his shit on them."

The result was an Oct. 29 report that shows a bear tripping over himself and spilling Halloween candy out of a pumpkin trick-or-treat bucket.

The effort to irritate the hackers is just the newest chapter in a broader Cyber Command effort to undermine foreign government cyber-operations. Cyber Command has been publishing samples of malicious software used by foreign hackers in recent years as part of an initiative aimed at getting the cybersecurity community to protect against adversaries' malware, thereby making the hacking less effective. The program is also aimed at sending a warning shot to foreign hackers that the U.S. government is tracking them.

Historically, this kind of taunting has been a way to boost morale at home, according to Pablo Breuer, the former director of U.S. Special Operations Command Donovan Group.

"When you go back to the heyday of information campaigns, go to World War II, and you look at the messaging governments did to their own populace, it was either a positive messaging about yourselves or it was negative messaging against the adversary," said Breuer, who previously worked at Cyber Command and the National Security Agency. "I think the silly graphics are more about messaging to the U.S. government and populace and branding: 'If the adversary is not that good, then Cyber Command must be really good.'"

Get silly

The first time Cyber Command wanted to share a mocking graphic about foreign hackers, the contractors had to redraft their sketches because the first one wasn't silly enough, the U.S. official said. The graphics company's task was to depict suspected Chinese government's malware, which Cyber Command called "Slothful Media" for its lazy coding techniques. In the end, when the command released the novel image, Cyber Command's Twitter followers reacted with jests and playful comments marveling at the portrayal.

"Our original graphic idea for 'Slothful Media' had to change because we realized it would be too cool," the official said, in recognition of the fact that the government runs the risk of unnecessarily inflating the adversary if the graphics are improperly executed. "Better to mock."

The official declined to share details about what made the original image too "cool," but the graphics company eventually produced an image of a cartoon-like sloth wearing headphones and crawling over to a laptop.

A relatively new implant, which we have dubbed #SlothfulMedia, has been used to target victims in a number of countries, including: India, Kazakhstan, Kyrgyzstan, Malaysia, Russia and Ukraine.

See more on @US_CYBERCOM's Virus Total page: https://t.co/HrPgvyPJ4v pic.twitter.com/b9hXnq2l6z

— USCYBERCOM Cybersecurity Alert (@CNMF_CyberAlert) October 1, 2020

The graphics program is just over a month old, during which time Cyber Command only exposed hacking operations from Russia and China. That means the command has not, to date, published teasing graphics about hackers from Iran and North Korea, two of the country's other chief digital adversaries.

Strategic aims

Dan Hoffman, a former chief of station at the CIA, told CyberScoop he thinks the publication of these graphics may not be overwhelmingly upsetting to Moscow or Beijing.

"You're definitely not going to influence the bad guys. They don't care," said Hoffman, whose tours of duty in the CIA included time in the former Soviet Union. "Maybe they don't like to be named and shamed but at the end of the day what Vladimir Putin would do at least is say … 'You named and shamed us? Ok we're gonna grab a shot of vodka and go back to work.'"

But the graphics tactic could be effective in signaling there may be harsher consequences down the road, Hoffman added. In recent years Cyber Command has been working to bolster the arsenal of responses it can use to deter foreign government hackers. The strategy, known as "persistent engagement," has led Cyber Command to shut down Russian social media trolls' internet access in one case, and in another, to send direct messages to Russian government actors to deter them from running election-related influence campaigns.

"They're talking about persistent engagement and that's what they're doing with the graphics — they're taking the fight to the enemy and saying if you're going to shoot at us we're going to go find and shoot you in the face so you can't shoot at us anymore," Hoffman said. "We don't want to go 'cyber nuclear war' with you … we'll shut you down at a playful level first with graphics, and we can escalate."

The cost of the cartoonish graphics alone, however, may not be great enough to change adversary behavior, according to Breuer.

"If Cyber Command is trying to send a message the adversary is trivial, the adversary is laughing on the way to the bank — because their cyber-operations are still remarkably successful," said Breuer, who now works at Cognitive Security Collaborative. "What real consequence is there to China and Russia from doing this? Compared to the value our adversaries are getting from these cyber-operations, they're just going to look at it as the cost of business."

Even if the graphics don't irk the foreign hackers, Cyber Command hopes they may prompt antivirus companies to pay more attention to the command's malware warnings, the U.S. official said.

"It increases engagement in the community, which gets more attention on the malware, so worse for the actors. Wins all around," the official said. "The community here is [having] fun with it, so that drives engagement on the stuff we want caught, and theoretically improves detection."

A Cyber Command spokesperson said the command "develops visual imagery to engage with the cyber security community on malware disclosures and vulnerability alerts. We recognize the key role that industry plays in ensuring global cybersecurity

defense against malicious cyber actors, and so we leverage social media best practices to enhance messaging with industry."